On the need for federated authorization in cross-organizational e-health platforms

Maarten Decat, Dimitri Van Landuyt, Bert Lagaisse, Wouter Joosen
iMinds-DistriNet, KU Leuven, 3001 Leuven, Belgium
first.last@cs.kuleuven.be

Keywords: E-health, security, access control, federated access control, authorization.

Abstract: Health care is currently witnessing increased specialization as well as a need for integrated care delivery. As a result, care organizations should collaborate and in order to facilitate this, e-health collaboration platforms are being created. Access control is a primary concern for such cross-organizational platforms and efficient access control management is crucial to their adoption. Federated access control is a potential technique to achieve this and our experience in multiple research projects shows that federated authorization is an essential building block for future collaboration platforms. However, this technology still faces open research challenges. This paper wants to spark research on these challenges by motivating the need for federated authorization in the context of a real-world collaborative care platform. Based on this case study, we also discuss the state of the art and present a set of key requirements to realize wide-scale adoption of federated authorization in practice.

1 Introduction

Health care is increasingly being delivered as a collaborative effort between multiple specialized care organizations and in order to facilitate this, collaborative e-health platforms are being created. For example, Vitalink (Vitalink, 2013) facilitates the sharing of medication and vaccinations of patients between medical professionals. Another example is OCareCloudS (OCareCloudS, 2014), a research project that aims to facilitate information sharing between the multiple organizations that provide home care to a certain care receiver.

A primary concern in these collaboration platforms is security. The data that are shared amongst the care organizations concern patients and as a result, data protection legislation applies. Cryptographic techniques can provide storage and transmission security, but in order to share data in a controlled way, application-level access control is required as well.

The goal of access control is to limit the access of *users* to the *resources* in the application by enforcing the *access control policies* of the organization that controls these resources (Samarati and de Vimercati, 2001). Access control is therefore highly interrelated with the user management of that organization: user accounts have to be created, access control policies have to be deployed and the access control data of users have to be managed. Examples of these data are the names of users, their roles in the organization, their birth date, their location, their department, their shifts, their assigned patients etc.

However, realizing access control for a collaboration platform is challenging because of the multiple organizations involved. These organizations often share the ownership of the data and should all be able to express their access constraints. However, these organizations remain separate domains in terms of administration and security, and do not necessarily trust each other completely. Amongst others, this leads to challenges such as sharing the identities of users between these organizations, integrating the multiple access control infrastructures, and evaluating the access control policies in a way that performs well and keeps the sensitive access control data of all organizations confidential. This paper is not the first to identify these challenges, e.g., (Poortinga-van Wijnen et al., 2010), but as we will show, not many of them have been addressed properly.

Federated access control is a potential answer to these challenges. While federated authentication is an established technology (e.g., (OpenId, 2013) and (SAML, 2005)), our experience with the OCareCloudS research project shows that *federated authorization* is necessary to address these challenges completely. Similar to federated authentication, federated authorization externalizes policy evaluation from an application. In the short term, this technique is re-

quired for the adoption of collaborative platforms by large organizations that require centralized user management. In the long term, it enables efficiently evaluation of cross-organizational policies while keeping sensitive access control data confidential.

However, while the concept of federated authorization is fairly intuitive, its realization still poses many challenges by itself, especially in realistic federations. Therefore, we want to spark research on federated authorization by motivating the need for it using the case study of the OCareCloudS collaboration platform. Although this paper focuses on a single case study, our research on federated authorization is based on and validated in multiple application domains (PUMA, 2014; SPARC, 2014).

The remainder of this paper is structured as follows: Section 2 describes the case study of the collaborative care platform. Section 3 illustrates the need for federated authorization in this case study. Section 4 extrapolates a set of key requirements for federated authorization. Section 5 concludes this paper.

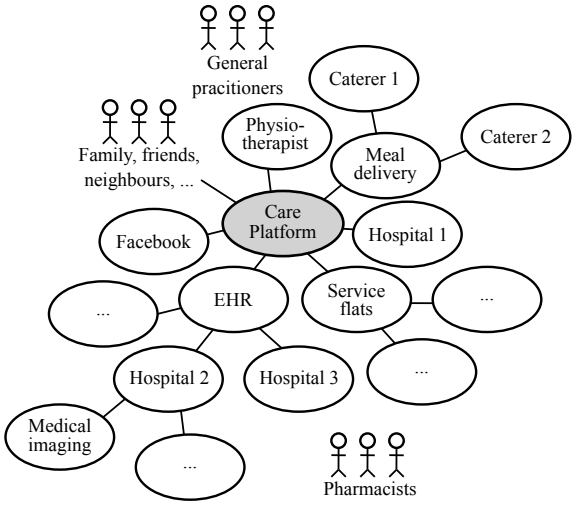

Figure 1: Part of the federation of organizations involved in the collaborative care platform. As shown, such a platform quickly leads to a federation of a large amount of organizations and individuals of different nature.

2 Case study: a collaborative care platform

The case study focuses on a software platform that aims to streamline home care by improving the communication between the multiple involved organizations. The platform therefore digitizes the information that these organizations share, such as prescriptions of and notes about the care receiver.

Together, the various organizations involved in the collaboration platform behave as a *federation*. This means that these organizations have set up collaboration agreements, but still remain separate domains in terms of security and administration, and do not necessarily trust each other completely.

Figure 1 illustrates the federation of organizations involved in the care platform. While this figure only illustrates a part of the complete federation, it already shows that a large amount of organizations is involved, such as general practitioner practices, elder homes, daily care organizations, physiotherapist practices, home nursing organizations, hospitals and catering services. Some of these are directly involved (e.g., the meal delivery service), but others get involved because of business relationships with directly involved organizations (e.g., the caterers) or because of the integration of the platform with the Electronic Health Record (EHR) for sharing patient data on a wider scale (e.g., other hospitals). Figure 1 also illustrates that the organizations in the federation are of very different nature, ranging from core-medical (e.g., general practitioners and hospitals) to supporting (e.g., caterers), and from large organizations (e.g., hospitals) to small organizations (e.g., a medical imaging practice) and even individuals (e.g., family, friends, general practitioners). Moreover, this federation is dynamic in the sense that new organizations can join the federation over time or others can leave.

The remainder of this section outlines the specific access control challenges that arise in the context of such large and complex federations.

2.1 Access control challenges

While the collaboration platform enables easier cross-organizational information sharing, the data in this platform are sensitive, personal and medical. Therefore, the platform should also enable more *controlled* information sharing. To achieve this, the collaboration platform performs *access control*, which limits the actions (e.g., read, write) that a user can take on a resource in the system (e.g., notes about the status of a patient) by enforcing access rules that are specified in *access control policies* (e.g., (OASIS, 2013)).

In the federation of the platform (see Figure 1), there are three types of access control policies:

1. *Intra-organizational*: Firstly, the care organizations want to constrain their own employees. For example, the hospital imposes that each of its nurses can only view data of care receivers explicitly assigned to him or her, which depends on internal task assignment.
2. *Inter-organizational*: Secondly, the care organi-

zations want to control which other organizations are allowed to access their data. For example, the hospital trusts the meal delivery service, but not a private hospital that also uses the platform.

3. *Cross-organizational*: Thirdly, the platform itself imposes access control polices that apply to all organizations and individuals using it. For example, these policies can impose that medical data can only be read by medical professionals that are not family members of the related patient, unless explicitly allowed by that patient.

Enforcing these policies in the federation requires collaboration because each of the involved organizations remains a separate domain of administration, i.e., each organization manages its own users and has its own access policies. As a result, the access control policies and the data required to evaluate them are spread over the multiple organizations. Consequently, multiple organizations are involved in evaluating these policies. Moreover, these organizations do not necessarily trust each other with their access control policies or data.

This collaborative decision making causes many challenges. Semantically, it leads to challenges such as how a single user can be identified as the same user by these multiple organizations, and how the policies of one organization can reason about the users of another organization while for example the meaning of the role "nurse" can differ substantially in different organizational contexts. Technically, it leads to challenges such as how the different user management and authorization infrastructures employed by the organizations can interact, and how this federated decision making can provide suitable performance if communication is required between multiple separate organizations. And in terms of trust, it leads to challenges such as expressing trust in the other organizations in the federation, allowing each organization to keep sensitive access control data confidential from organizations it does not trust, and achieving correct decision making while the trustworthiness of the data received from another organization can vary, e.g., Facebook versus a university hospital.

Prior to this work, other authors have also discussed challenges for access control in a federated context (e.g., (Colombo et al., 2010; Freudenthal et al., 2002; Poortinga-van Wijnen et al., 2010; Chakraborty and Ray, 2006)). However, a large part of these challenges still remains and our experience shows that the technique of federated authorization is a necessary building block to address these. However, this technique still poses challenges by itself. Therefore, this paper focuses on the need for federated authorization in order to spark research on this topic.

3 The need for federated authorization

As mentioned, we believe that federated authorization is an important enabler for access control for future collaborative applications. In the short term, federated authorization is necessary to enable organizations to effectively enforce their intra-organizational policies on remote applications such as the care platform. In the long term, federated authorization is necessary to address the challenges related to performance and confidentiality of policy evaluation across the federation.

Let us start by illustrating the need for federated authorization in the short term. To do this, we focus on a simplified version of the complete federation consisting of three organizations (see Figure 2): (i) a small physiotherapist practice that helps care receivers with physical exercises, (ii) a mid-size meal delivery service that delivers hot meals on a daily basis and (iii) a large hospital that is responsible for medical examinations and treatments. As said, these three organizations collaborate via the care platform. For example, the meal delivery service visits care receivers most often and can notice that they are not eating well or are complaining about the effects of their medication. This is important information that should be shared with the other organizations.

For the point of all three care organizations the care platform behaves as a remote web application: the data in the application are located outside of the premises of the organizations and the platform is accessed using a web-based interface. However, the three organizations involved in this example are very different in terms of how they typically manage their own users for this remote application: (i) The physiotherapist practice is a small organization of only three physiotherapists and does not have IT infrastructure yet. Therefore, it chooses to define and manage their user accounts on the platform itself. As a result, the platform also hosts the user data of the physiotherapist practice. While this approach duplicates user data

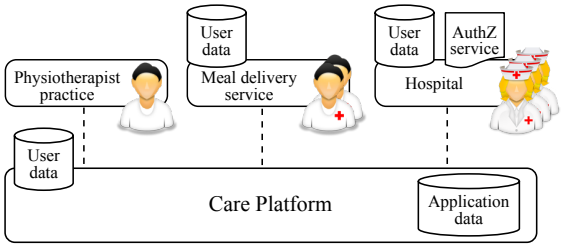

Figure 2: A simplified version of the federation of organizations involved in the collaborative care platform consisting of three organizations of different size.

for every application that the physiotherapist practice employs, the resulting management overhead is limited because of the small size of the practice. (ii) The meal delivery service on the other hand is larger than the physiotherapist practice. It employs around thirty caregivers and utilizes its own centralized user management infrastructure for assigning care receivers to care givers and managing paychecks and holidays. (iii) Finally, the hospital is the largest organization of the three. It employs over three hundred nurses and physicians. The hospital utilizes a similar infrastructure for user management as the meal delivery service, plus a central authorization service for all its applications. Both the meal delivery service and the hospital would like to integrate their existing infrastructures with the platform in order to conserve their efficient management. For example, adding a new user or access rule should only require changes to be made in exactly one place.

Integrating the collaboration platform with the user management infrastructures of the meal delivery service and the hospital can be achieved using federated authentication techniques (SAML, 2005; OpenId, 2013). Authentication is the part of access control that confirms the stated identity of a user, for example by checking the combination of a username and password. Federated authentication externalizes authentication from the platform as shown in Figure 3. As a result, the user data of the meal delivery service and the hospital are also externalized from the platform and can be centralized for all the applications they employ. Moreover, sensitive data such as user passwords are not shared with the platform.

However, user management is only part of the complete access control management. After users have been defined, the organizations have to specify the access policies that constrain them. Traditionally, these policies are deployed on and evaluated by the platform. This approach has the following disadvantages:

- It requires the platform to provide an access control infrastructure sufficiently expressive to support all rules of all organizations potentially involved in the federation.
- It requires an organization to specify its policies for every application it employs. This hinders a new organization to join the federation because of the larger initial management overhead and increased authorization management afterwards.
- It forces the organization to disclose its policies and the data required to evaluate them. These policies may be sensitive because they reason about competitors, and these data may include internal information of the organization, which is sensitive for competitive reasons, or even patient data, which are sensitive for privacy reasons.

Similar to user management, the increased authorization management required for this approach is not practically feasible for an organization of the size of the hospital, which requires to reuse or at least integrate its centralized authorization infrastructure. Moreover, independent of the size of the organization, the necessary disclosure of sensitive policies and user data either limits the expressiveness of these policies or hinders the adoption of the platform itself.

Federated authorization can address these disadvantages, as it externalizes policy evaluation from the application similarly to federated authentication (see Figure 4). As a result, federated authorization relieves the platform of the burden to provide a generic and complex access control infrastructure. Federated authorization also lowers the initial administration overhead when a new organization joins the platform since existing policies and user accounts can be reused. Moreover, federated authorization conserves the centralized administration of the hospital, even when using remote applications. Finally, federated authorization enables the hospital to enforce access control on

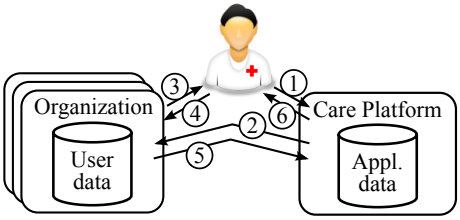

Figure 3: High-level overview of *federated authentication*: when the user make a request to the platform (step 1), the platform asks the organization of the user for an authentication statement (step 2). This organization authenticates the user locally (e.g., by asking for his password, steps 3 and 4) and returns the identity of the authenticated user to the platform afterward (step 5).

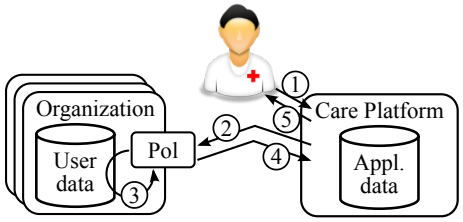

Figure 4: High-level overview of *federated authorization*: When a user makes a request to the platform (step 1), the platform asks the organization of the user for an access control decision (step 2). This organization evaluates its policies locally (step 3) and returns its decision (step 4), which the platform enforces afterward.

the platform without having to disclose its policies or the data required by them. The main disadvantage of federated authorization is its complexity. However, the value of the four benefits listed above grows with the size of the organization. Federated authorization therefore is an important enabler for the adoption of collaborative e-health platforms (and more generally, remote applications) by large organizations.

As such, this scenario illustrates the need for federated authorization for enforcing the intra-organizational policies of an organization on remote applications. This technique can also be applied to more complex policies and usage scenarios in the federation. For example, the cross-organizational policies imposed by the platform itself require access control data spread over multiple organizations. For these policies, federated authorization enables an organization to evaluate their part of the complete policy without having to share the data required for this. This approach can also improve performance of cross-organizational policy evaluation by evaluating parts of a policy close to the data they require instead of transporting the data itself, which is especially relevant if the organizations in the federation have separate IT infrastructures. As such, federated authorization is a necessary building block for federated access control in both short and long term.

4 Key requirements for federated authorization

The previous section has motivated the need for federated authorization in the context of a collaborative care platform. Federated authorization has been discussed by other authors, e.g., (Poortinga-van Wijnen et al., 2010), and initial attempts have been made to create supporting run-time environments, e.g., (Decat et al., 2013; Lischka et al., 2009). Moreover, simple domain-specific instances of federated authorization are already used in practice, e.g., for credit card payments where the bank of the customer is contacted to authorize the payment. However, while the basic concept of federated authorization is fairly intuitive, many open research challenges still remain before it can be realized in a practical setting, amongst others because of the complexity of real-life federations as described in Section 2.1. In the remainder of this section, we discuss our key requirements for federated authorization in terms of policy language support, run-time support and standardization.

Policy language support. Existing policy languages such as XACML (OASIS, 2013) already provide extensive constructs for specifying access rules within a single organization. However, these languages and their underlying models should be extended to support federated authorization. Firstly, policies should be able to refer to other organizations in the federation and incorporate the result of their policy evaluation. This basic requirement has been addressed by previous research (Lischka et al., 2009; Decat et al., 2013). Secondly, these policy languages should also be extended to support reasoning about other organizations as a whole. For example, organizations should be able to express their trust in other organizations in the federation and incorporate this trust in their access decisions. Thirdly, since realistic federations can be large and members can join and leave frequently, these policies require language mechanisms that make abstraction of specific members of the federation, e.g., higher-level federation roles such as “home care provider”, “caterer” or “hospital”. As such, existing paradigms such as role-based access control (Ferraiolo et al., 2001) and attribute-based access control (Jin et al., 2012) can serve as a first step to address these challenges.

Run-time support. Next to specifying policies for federated authorization, a supporting run-time execution environment is required, with at its core the policy engine. In terms of policy evaluation, federated authorization requires these engines to be able to contact the engines of other organizations. Again, this basic requirement has already been addressed in literature (Lischka et al., 2009; Decat et al., 2013). However, employing federated authorization in practice requires additional features of policy engines. For example, by employing federated authorization, policies are also evaluated in a distributed fashion. If these policies have side-effects (e.g., obligations (OASIS, 2013)), some form of concurrency control is required to ensure correctness. Moreover, while federated authorization can be employed as a performance tactic, it still entails communication with a remote organization. Therefore, it requires performance tactics itself to keep its latency low, e.g., decision caching, caching of access data or policy splitting. Since access control is a security feature, the proven correctness of each of these tactics is essential.

Interoperability through standardization. Cross-cutting to the above, standardization is key to the successful adoption of federated authorization, especially to achieve dynamic and large-scale federations. More precisely, federated authorization requires standardized policy languages, data sharing formats and access control orchestration mechanisms.

Initial steps in this direction are currently being made, e.g., by the OASIS working group on cloud authorization (CloudAuthZ, 2013).

5 Conclusion

In this paper, we motivated the need for federated authorization in the context of a collaborative care platform. Federated authorization is a technique to externalize policy evaluation from an application. Federated authorization is a necessary building block for access control in the federations of organizations that arise from current and future inter-organizational collaboration platforms. In the short term, this technique can facilitate the adoption of collaborative platforms by large organizations which require centralized user management. In the long term, this technique can be employed to evaluate cross-organizational policies efficiently while keeping sensitive data confidential. Although this paper mainly focused on a single collaborative e-health platform, our interactions with industry partners have confirmed the need for federated authorization in other domains that rely on inter-organizational collaboration, such as electronic document processing (PUMA, 2014) and payment services (SPARC, 2014). However, while the concept of federated authorization is fairly intuitive, there are still research challenges that should be addressed to achieve wide-spread adoption. We will continue our work on these challenges and hope that this position paper has sparked the interest of other researchers.

Acknowledgments. This research is partially funded by the Research Fund KU Leuven, by the EU FP7 project NESSoS and by the Agency for Innovation by Science and Technology in Flanders (IWT). With the financial support from the Prevention of and Fight against Crime Programme of the European Union (B-CCENTRE).

REFERENCES

Chakraborty, S. and Ray, I. (2006). TrustBAC: integrating trust relationships into the RBAC model for access control in open systems. In *SACMAT*, pages 49–58. ACM.

CloudAuthZ (2013). OASIS Cloud Authorization (CloudAuthZ) TC | OASIS. https://www.oasis-open.org/committees/cloudauthz/.

Colombo, M., Lazouski, A., Martinelli, F., and Mori, P. (2010). Access and usage control in grid systems. In *Handbook of Information and Communication Security*.

Decat, M., Van Landuyt, D., Lagaisse, B., Crispo, B., and Joosen, W. (2013). Federated authorization for software-as-a-service applications. In *To be published in the proceedings of DOA-Trusted Cloud'13*.

Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D., and Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *TISSEC*, 4(3):224–274.

Freudenthal, E., Pesin, T., Port, L., Keenan, E., and Karamcheti, V. (2002). dRBAC: distributed role-based access control for dynamic coalition environments. In *DSS*, pages 411–420.

Jin, X., Krishnan, R., and Sandhu, R. (2012). A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. In *Data and Applications Security and Privacy XXVI*, pages 41–55. Springer Berlin Heidelberg.

Lischka, M., Endo, Y., and Sánchez Cuenca, M. (2009). Deductive policies with xacml. In *Proceedings of the 2009 ACM workshop on Secure web services*, pages 37–44. ACM.

OASIS (2013). eXtensible Access Control Markup Language (XACML) Version 3.0.

OCareCloudS (2014). OCareCloudS - Overview projects - iMinds. http://www.iminds.be/en/research/overview-projects/p/detail/ocareclouds-2.

OpenId (2013). OpenID Authentication 2.0 - Final. http://openid.net/specs/openid-authentication-2_0.html.

Poortinga-van Wijnen, R., Hulsebosch, B., Reitsma, J., and Wegdam, M. (2010). Federated authorisation and group management in e-science.

PUMA (2014). Permission, User Management and Availability for multi-tenant SaaS applications (PUMA). http://distrinet.cs.kuleuven.be/research/projects/PUMA.

Samarati, P. and de Vimercati, S. C. (2001). Access control: Policies, models, and mechanisms. In *Foundations of Security Analysis and Design*, pages 137–196. Springer.

SAML (2005). Security Assertion Markup Language (SAML) v2.0. http://www.oasis-open.org/standards#samlv2.0.

SPARC (2014). Smart Plug-in Automobile Renewable Charging Services (SPARC). https://distrinet.cs.kuleuven.be/research/projects/SPARC.

Vitalink (2013). Home | Vitalink. http://www.vitalink.be/.